AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ronald Morin, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

1. I have been employed as an HSI Special Agent since May of 2006, and am currently assigned to the Manchester, New Hampshire Resident Office. Prior to my employment with HSI, I served as a Police Officer in the State of Maine. As part of my regular duties as a Special Agent, I am tasked with the investigation of criminal violations related to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A (the "Specified Federal Offenses"). I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, to include digital/computer media. During the course of this investigation I have conferred with other investigators who have conducted numerous investigations and executed numerous search warrants which involved child exploitation and/or child pornography offenses. I have previously obtained federal search warrants related to child pornography offenses and have participated in the execution of numerous search warrants, many of which involved child pornography offenses.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a search warrant authorizing a search of a residence located at 57 Blueberry Lane, Apartment 28, Laconia, NH 03246 (the "Premises"), as further described in Attachment A. I seek to seize evidence, fruits, and

instrumentalities of the Specified Federal Offenses, which relate to the knowing possession and distribution of child pornography. I request authority to (i) search the entire Premises and any computer and computer media (as defined in this affidavit) located therein and where the items specified in Attachment B may be found and (ii) seize any and all items listed in Attachment B as instrumentalities, fruits, and evidence of the Specified Federal Offenses.

4. The statements in this affidavit are based on information provided by other law enforcement officers, and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. While I have included all material facts relevant to the requested search warrant, I have not set forth all of my knowledge about this matter.

5. The first section of this affidavit recites the statutory language and definitions for the relevant Specified Federal Offenses. The second section of the affidavit provides background on computers and child pornography in general and details the process involved in the search and seizure of computer systems. Finally, the third section of the affidavit sets forth the probable cause to believe that (i) the Specified Federal Offenses have been committed; and (ii) that evidence, fruit, and instrumentalities of the Specified Federal Offenses are likely to be found in the Premises, respectively.

SECTION I. STATUTORY LANGUAGE AND DEFINITIONS

A. STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252, and 2252A relating to the sexual exploitation, and material involving the sexual exploitation, of minors. The relevant statutes are recited in pertinent part as follows:

a. 18 U.S.C. § 2251(a) states that it is unlawful for any person to employ, use, persuade, induce, entice or coerce any minor to engage in, or transport any minor in or affecting interstate commerce, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

b. 18 U.S.C. § 2252(a)(2) states that it is unlawful for any person to knowingly receive, or distribute, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in interstate or affecting interstate commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct, and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(4)(B) states that it is unlawful for any person to knowingly possess, or knowingly access with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct, and such visual depiction is of such conduct.

d. 18 U.S.C. Section 2252A(a)(2) states that it is unlawful for any person to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. Section 2252A(a)(5)(B) states that it is unlawful to knowingly possess, or knowingly access with the intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been

mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

B. DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. "Child Pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

c. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

e. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

h. "Sexually explicit conduct" as used in this affidavit applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. §2256(8)(C). In those contexts, the term refers to actual or simulated sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

i. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image; and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

j. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

SECTION II. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY; SPECFICS OF COMPUTER SEARCHES/SEIZURES

A. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced, possessed, and distributed.

9. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking. With digital cameras, images of child pornography can be transferred directly onto a computer; in addition, the use of commercially available software and devices also allows for the conversion and transfer of other forms of visual media into various digital and electronic media formats. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet affords individuals several different venues for meeting and communicating with each other; and obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. The Internet is also used as a means for child sexual exploitation offenders

to solicit potential victims through the use of various online services to include, but not limited to, online profiles, email, and instant messaging and chat.

12. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP (Internet Service Provider) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet

directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

13. File transfers and online connections occur to and from IP (Internet Protocol) addresses. These addresses, expressed as four sets of numbers separated by decimal points, are unique to particular computers during online sessions. An IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers.

14. Third-party software is available to identify the IP address of a particular computer during an online session. Such software monitors and logs Internet and local network traffic. It is possible to identify the person associated with a particular IP address through ISP records. ISPs maintain records of the IP addresses used by the individuals or businesses that obtain Internet connection service through the ISP. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

15. I also know that individuals who possess and share child pornography often keep it and the electronic devices they use to do it in their residences and vehicles. They may keep child pornography on devices like flash drives which are small and can be easily hidden. They often also access child pornography on cellular devices that can be kept on their persons, in their cars, or in their residences.

B. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

16. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

17. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware

drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

18. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. Sections 2251 through 2256, I request authority to seize them all as such.

SECTION III. PROBABLE CAUSE

19. On 1/18/2019 I received information from HSI SA Sara Seidman, Liaison at the National Center for Missing and Exploited Children (NCMEC), regarding CyberTipline Report# 45679110, pertaining to possible child sex trafficking. SA Seidman received the report from Norsung Wodhen, Analyst at NCMEC.

20. On 1/17/2019, NCMEC received a CyberTipline report which NCMEC designated as #45679110 from Skout.com (hereafter "SKOUT"), The Meet Group Legal Team, 100 Union Square Drive, New Hope, Pennsylvania (PA). SKOUT is the developer of a location-based social networking and dating application and website. SKOUT is available on both iOS and Android operating systems. SKOUT uses a cellphone's global positioning system to help users to find other users within a general radius of one another.

21. SKOUT reported to NCMEC that a SKOUT user was attempting to meet another SKOUT user as part of a plan to have sex with a seven (7) year old girl. SKOUT identified the possible child victim "Sammi" associated with SKOUT ID# 142435075, email address titsntats420x@gmail.com and IP address 209.42.155.219 (login). Publicly available information indicates that the IP address geolocates to the area of Tilton, NH, and the internet service provider is Atlantic Broadband (Quincy, MA).

22. On 01/25/2019, SA Seidman provided me with CyberTipline Report# 45679110 which included communications between the SKOUT users on 12/25/ 2018 and 12/26/2018; SKOUT user profiles which included IP logs; and eight (8) still images in which the users sent. The images are described as:

a. Three (3) images depicting an adult Caucasian male's pelvic area with his penis exposed.

b. One (1) image depicting a Caucasian female's pelvic area with her vagina exposed and an object inserted into her anus. It is difficult to determine an approximate age of this female.

c. One (1) image (caption: "Kim 15's picture") depicting a Caucasian female giving fellatio to an animal.

d. One (1) image depicting a Caucasian female wearing a black t-shirt (white lettering on the back) and white panties (with unknown print) bent over at the waist. The female has pig tails with pink hair ties. A light blue shower curtain depicting the phrase "so you come here often".

e. One (1) image depicting a prepubescent Caucasian female lying on her back on a tan couch. There is a multi-colored blanket beneath her. The child is wearing a pink tank top with multi-colored stripes near the top, and black lace panties. The child has a lollipop in her mouth.

f. One (1) image depicting multi-colored artwork.

23. On 01/28/2019, I issued a DHS Summons (ICE-HSI-MF-2019-00187) to Atlantic Broadband for subscriber records for IP address 209.42.155.219 on 12/25/2018 @ 21:41:06 UTC. On 01/31/2019, Atlantic Broadband (Subsento) provided records identifying subscriber:

Stephanie Stephens
57 Blueberry Lane, Apartment 28, Laconia, NH 03246
[redacted]
Visa, x5173, Exp.: 12/2020
Account Activation Date: 05/17/2018. The account was still active as of April 16, 2019.

24. On 01/28/2019, I prepared a DHS Summons (ICE-HSI-MF-2019-00189) for subscriber records for email address titsntats420x@gmail.com. On 02/01/2019, I obtained a Non-Disclosure Court Order for email addresses titsntats420x@gmail.com. On 02/15/2019, I received subscriber records from Google identifying the following:

> Name: Tyler Payne
> Email: titsntats420x@gmail.com
> Created: 11/25/2018 at 22:02:54 UTC
> IP Address: 209.42.155.219
> Google Account ID: 479756484904
> The IP address identified by SKOUT is the same IP address listed by Google.

25. On 02/01/2019, I conducted database checks on Stephanie Stephens. Consolidated Lead Evaluation and Reporting (CLEAR) Records indicate that Stephanie Stephens has DOB: [redacted], SSN: [redacted] with the address 57 Blueberry Lane, Apartment 28, Laconia, NH. There were no criminal records identified for Stephanie Stephens.

26. On 02/01/2019, I contacted Laconia Police Department (LPD) to inquire about Stephanie Stephens. Detective Sergeant Benjamin Black provided LPD records associated with Stephanie Stephens. SGT Black advised that Stephanie Stephens has a son, Coen Maynor, DOB: [redacted].

27. On 02/01/2019, I conducted open source checks on Stephanie Stephens. I viewed Stephanie Stephens' Facebook page which indicates she is "in a relationship" with Thomas Goupil (hereafter "Goupil"). The Facebook page also indicates that Stephanie Stephens works as a dietary aid at Belknap County Nursing Home which is located at 30 County Drive, Laconia, New Hampshire.

28. On 02/01/2019, I conducted database checks on Goupil. CLEAR Records indicate that Goupil has DOB: [redacted], SSN: [redacted], with the address 36 Haggett Farm Road, Northfield, NH. Goupil has telephone number [redacted] associated to him. This number is

associated to the IP address used to login to SKOUT on 12/25/2018. Goupil has FBI# [redacted] with drug related criminal offense history.

29. On 02/01/2019, I contacted Northfield PD for information relating to Goupil. There was no relevant information identified.

30. On 02/01/2019, I conducted open source checks on Goupil. Goupil's Facebook page indicates that Goupil is "in a relationship" with Stephanie Stephens. Facebook records also indicate that Goupil works as a chef at the Belknap County Nursing Home which is located at 30 County Drive, Laconia, New Hampshire.

31. On 02/04/2019, I submitted a DHS Summons (ICE-HSI-MF-2019-00201) to US Cellular for subscriber information on 603-393-7914, the telephone number associated with IP address used for the SKOUT logins. On 02/05/2019, US Cellular provided subscriber records for telephone number 603-393-7914 identifying:

> Thomas Goupil
> 36 Haggett Farm Road, Northfield, NH 03276
> Effective date: 03/09/2017 @ 23:59:59 CST
> Device: Samsung Galaxy S7 black
> MIN: 6034199079
> TMSI: 311580706264968

32. On 02/07/2019, I requested and received NH Driver's License (DL) photo and Registration information for Stephanie Stephens and Goupil. Goupil has a silver 2010 Chevrolet 1500 pick-up truck bearing NH Registration "GOUPIL" in his name. Stephanie Stephens does not appear to have a NH driver's license or any vehicles registered to her.

33. On 02/12/2019, I and HSI SA Michael Perrella conducted surveillance of 57 Blueberry Lane, Apartment 28, Laconia, NH (the PREMISES). Special Agents observed Goupil's vehicle parked in front of the residence.

34. On 02/12/2019, I received an email from LPD SGT Black indicating that they had received a NCMEC CyberTip relating to the PREMISES from Tilton Police Department (TPD) SGT Nathan Buffington.

35. On 02/13/2019, I contacted TPD SGT Buffington who advised that they received NCMEC CyberTip# 45415902 relating to a Tumblr (here after "TUMBLR") account used to upload one (1) image of child pornography. TPD Detective Christopher Rideout obtained two State Search Warrants; one for records relating to the TUMBLR account identified in CyberTip #45415902, and one for subscriber information for the associated IP address. Atlantic Broadband records identified that the IP address is associated to the PREMISES in Laconia, NH.

36. On 02/14/2019, I met with Detective Sergeant Nathan Buffington at Tilton Police Department (TPD) and obtained a copy of their case (19-1666-OF). I reviewed NCMEC CyberTip# 45415902 and the TPD case.

37. On 02/06/2019, the TPD received CyberTipline Report #45415902 from the National Center for Missing & Exploited Children (NCMEC). The CyberTipline report was submitted to Tilton PD via the NH ICAC Task Force and reviewed by Detective Christopher Rideout.

38. Detective Rideout reported that on 02/15/2019, Emily McKeon of the electronic service provider TUMBLR discovered that one of its users posted possible child sexual abuse images to a blog on their website.

39. One (1) digital photograph (.jpg file) was included with the CyberTipline report. According to the report, this file is a representative sample of the possible child sexual abuse images uploaded to a blog on TUMBLR. The images were uploaded to the TUMBLR URL "slutbitchs420.tumblr.com" by someone using the Screen/User Name "slutbitchs420". The CyberTipline report includes an IP Log, which indicates that file was uploaded approximately

0328 EST on 11/25/2018 via IP Address 209.42.155.219 (the PREMISES). Tumblr provided the following email address for the "slutbitchs420" account: budnboobs420@gmail.com.

40. The following briefly describes the photograph uploaded to the "slutbitchs420" blog:

File "messaging_media_l.jpg" depicts a naked prepubescent female. She is wearing only a t-shirt which covers her undeveloped breasts and is laying on her back on top of a blue blanket. She is seen using her right hand to grab an adult males' penis and her legs are spread, which depicts her vagina and penis as the focal point of the image. Only the adult males' penis and lower part of his shirt can be seen. This image is attached as EXHIBIT A.

41. The IP Address 209.42.155.219 resolved back to Atlantic Broadband. The IP address geo-locates back to Tilton, New Hampshire. On February 7th, 2019, TPD Detective Rideout applied for and was granted a search warrant of Atlantic Broadband, asking for subscriber records for IP Address 209.42.155.219.

42. On 02/07/2019, TPD Detective Rideout applied for and was granted a search warrant of TUMBLR, asking for all account information for bunboobs420@gmail.com, budnboobs420, slutbitches420.tumblr.com, and slutbitches420.

43. On 02/08/2019, TPD Detective Rideout received via email the results of my search warrant of Atlantic Broadband from Subsentio who is the custodian of records for Atlantic Broadband. The subscriber information for IP address 209.42.155.219 on 11/25/2018 showed as:

Stephanie Stephens
DOB: [redacted]
57 Blueberry Lane, Apartment. 28, Laconia, NH 03246
SS#[redacted]

44. The account number for Stephanie Stephens is 8282160060310517 with a visa credit card used as payment. Stephanie Stephens's account was activated on 05/17/2018 and was still active as of February 8, 2019.

45. On 03/05/2019, I received an email from LPD SGT Black indicating that they received additional CyberTipline Reports from the National Center for Missing and Exploited Children (NCMEC) relating to the PREMISES, 57 Blueberry Lane, Apartment 28, Laconia, NH. Their investigation also identified a possible suspect of Mason STEPHENS (hereafter "STEPHENS"), DOB: [redacted] (27yo). I viewed STEPHENS' Facebook page which indicates that Mason STEPHENS is the Brother of Stephanie Stephens.

46. On 03/05/2019, NH Internet Crimes Against Children (ICAC) Task Force Commander SGT John Perrachi forwarded the following six (6) NCMEC CyberTipline Reports to me relating to Stephanie Stephens's IP address:

a. CyberTipline Report# 47030918 was received by NCMEC on 02/23/2019 from MeetMe.com (hereafter "MeetMe"), MeetMe Inc. Legal Team, 100 Union Square Drive, New Hope, PA. The Company (The Meet Group) is a portfolio of mobile social entertainment apps. Its primary apps are MeetMe, LOVOO, SKOUT, and Tagged. The Company has millions of mobile daily active users. Its apps are available on iPhone, iPad, and Android in multiple languages. Through these apps, users can stream live video, send gifts, chat, and share photos. MeetMe reported that a user uploaded one (1) apparent image of child pornography. The image was uploaded on 02/22/2019 by user "Tasha" (associated email address mayhemmason420@gmail.com) from IP address 209.42.155.219 (the PREMISES). The image was viewed by a SKOUT staff member. The image depicts a female lying on her back with her vagina and anus exposed. It is difficult to determine the age of the female depicted in the image. The Subscriber of the IP Address associated with the CyberTipline Report is Stephanie Stephens. MeetMe provided SKOUT profile images of "Tasha" which depict an adult Caucasian female. Mason STEPHENS' Facebook page indicates that he has an associate named Saralynn CASTILLOUX (hereafter "CASTILLOUX) and displays images that appear to match the SKOUT profile images of "Tasha".

b. CyberTipline Report# 47030263 was received by NCMEC on 02/23/2019 from MeetMe.com. MeetMe reported possible possession, manufacture, and/or distribution of

illegal content. On 02/21/2019 a suspect image was uploaded by user "Tasha" (mayhemmason420@gmail.com) from IP address 209.42.155.219 (the PREMISES). The image was viewed by a SKOUT staff member. The image depicts a MINOR Caucasian female lying on her back on a tan couch. There is a multi-colored blanket beneath her. The child is wearing a pink tank top with multi-colored stripes near the top, and black lace panties. The child has a lollipop in her mouth (this is the same image as contained in NCMEC CyberTipline Report# 45679110, referenced in paragraph #22e above). MeetMe provided SKOUT profile images of "Tasha" which depict images consistent with CASTILLOUX.

c. CyberTipline Report# 47029645 was received by NCMEC on 02/23/2019 from MeetMe.com. MeetMe reported that a user uploaded one (1) apparent image of child pornography. The image was uploaded on 02/21/2019 @ 06:07:39 UTC by user "Tasha" (mayhemmason420@gmail.com) from IP address 209.42.155.219 (the PREMISES). The image depicts a Caucasian female child (approximately 5-7 years old) with an erect penis in her mouth. The child is holding a piece of paper with the phrase "I (heart) love cum". The image was viewed by a SKOUT staff member. This image is attached as Exhibit B.

d. CyberTipline Report# 47028898 was received by NCMEC on 02/23/2019 from MeetMe.com. MeetMe reported possible child sexual molestation. An image of child pornography was uploaded on 02/21/2019 @ 19:46:24 UTC by user "Tasha" (mayhemmason420@gmail.com) from IP address 209.42.155.219 (the PREMISES). The uploaded image is the same image contained in Exhibit B. The image was viewed by a SKOUT staff member. SKOUT provided chat that was associated with the posted images. In the chat, "Tasha" asks,"U ever fuck wit anyone under 18?" "Tasha" also states in the communications: that she is 15 years old, from New Hampshire, and "fucked" a 9-year-old.

e. CyberTipline Report# 47023468 was received by NCMEC on 02/23/2019 from MeetMe.com. MeetMe reported possible child sexual molestation. On 02/21/2019 a suspect image was uploaded by user "Tasha" (mayhemmason420@gmail.com) from IP address 209.42.155.219 (the PREMISES). The image was viewed by a SKOUT staff member and is the same image referenced in paragraphs 22(e) and 46(b) above. The NCMEC lead information included the Kik profile of "Mason Stevens (sp)/mayhemmason420" with an image depicting Mason STEPHENS, DOB: 01/04/1992.

f. CyberTipline Report# 43568138 was received by NCMEC on 11/26/2018 from Facebook (Jason Barry),1601 Willow Road, Menlo Park, CA. Facebook reported the receipt of one (1) image of apparent child pornography on 11/25/2018 @ 04:23:19 UTC at the IP address 209.42.155.219 (the PREMISES) via Facebook Messenger. The image is the same as contained in Exhibit A. The image was viewed by Facebook. The report identifies the recipient was Mason STEPHENS, DOB: 01/04/1992 with email address mayhemmason420@gmail.com (verified).

47. On 04/05/2019, I issued a DHS Summons (ICE-HSI-MF-2019-00427) to Atlantic Broadband for subscriber information for IP address 209.42.155.219 on 11/24/2018 @ 20:23:19 PST, 02/21/2019 @ 06:29:43 UTC, and 02/21/2019 @ 19:46:24 UTC (dates and times of the uploads of images of child pornography). On 04/15/2019, Atlantic Broadband (Subsentio) provided records identifying the subscriber as:

> Stephanie Stephens
> 57 Blueberry Lane, Apartment 28, Laconia, NH 03246
> Activation Date: 05/17/2018 (still active as of 4/14/2019)
> [redacted]
> Payment: [redacted]

48. On 04/05/2019, I prepared a DHS Summons (ICE-HSI-MF-2019-00426) for subscriber records for email addresses mayhemmason420@gmail.com and budnboobs420@gmail.com from 11/15/2018 to present. On 04/12/2019, I obtained a Non-Disclosure Court Order for email addresses mayhemmason420@gmail.com and budnboobs420@gmail.com. On 05/15/2019, Google provided records indicating the subscriber of mayhemmasaon420@gmail.com is Mason STEPHENS. There were no IP logs provided. The subscriber of budnboobs420@gmail.com is "Nico Ticks" with logins dated from 11/18/2018 to 01/13/2019 from IP address 209.42.155.219 (the PREMISES).

49. On 04/17/2019, I and SA Perrella conducted a knock and talk at 57 Blueberry Lane, Apartment 28, Laconia, NH. Special Agents made contact with Stephanie Stephens. Using a ruse, I inquired about who resided at the address. Stephanie Stephens advised that she resided at the address with her son (MINOR). Special Agents noted that a vehicle bearing NH Registration "GOUPIL" was parked in front of the address.

50. On 04/19/2019, I submitted a DHS Summons (ICE-HSI-MF-2019-00454) to Facebook for Subscriber and IP logs for www.facebook.com/mason.stephens.3344 from 11/24/2018 to

present. On 04/23/2019, Facebook provided records indicating the subscriber of the account "mason.stephens.3344" is Mason STEPHENS. The registered email on the account is mayhemmason420@gmail.com. Facebook provided IP logins from 12/02/2018 to 03/08/2019 and logouts from 12/01/2018 to 04/12/2019 from IP address 209.42.155.219 (the PREMISES).

51. On 04/29/2019, HSI Special Agent (SA) Ronald Morin submitted three (3) images to NCMEC to be reviewed for identified children. Two (2) of the images appear to be child pornography. These images are related to the NCMEC reports associated to the IP address 209.42.155.219, subscribed to by Stephanie STEPHENS, 57 Blueberry Lane, Apartment 28, Laconia, NH and the possession/distribution of child pornography.

52. .On 05/15/2019 NCMEC provided Child Identification Report (CIR)# 123118 indicating that image "messaging_media_1.jpg" is part of the known series "AtSea" (attached as Exhibit A) and image "47029645.PNG" (top image) is part of the known series "Jewelry1" (attached as Exhibit B). Additionally, NCMEC provided ECD Technical Assistance notes identifying five (5) additional related CyberTips (45690404, 47435362, 47029044, 43568130, and 45679176). I requested copies of these CyberTips. NCMEC provided me with CyberTips 45690404, 47435362, 47029044, 43568130, and 45679176. I reviewed these CyberTips and identified:

a. CyberTipline Report# 45690404 was received by NCMEC on 01/17/2019 from Skout.com. SKOUT reported possible possession, manufacture, and/or distribution of illegal content. On 12/20/2019 two (2) suspect images were uploaded by user "Sammi" (budnboobs@gmail.com) from IP address 209.42.155.219 (the PREMISES). The images were viewed by a SKOUT staff member. I reviewed the images included in this report and identified two (2) images of child pornography. One image is from the known series "AtSea" (Exhibit A)and the other image is of what appears to be a prepubescent boy with an erect adult male penis in his mouth. The boy is holding the penis with his left hand. There appears to be semen on the adult male's penis. This image is attached as EXHIBIT C. A third image depicts an adult female from the waist up, with her naked breasts exposed. This image appears to be consistent with Facebook images of Stephanie Stephens.

b. CyberTipline Report# 47435362 was received by NCMEC on 03/09/2019 from Facebook. Facebook reported possible possession, manufacture, and/or distribution of illegal content. On 03/08/2019 @ 10:20:18 UTC one (1) suspect image was uploaded by user steph.kuntz.90 (budnboobs420@gmail.com) from IP address 209.42.155.219 (the PREMISES). The image was viewed by Facebook staff. I reviewed the image which depicts a prepubescent female with the focal point of the photo being her vagina and anus. The child is spreading open her vagina with her hands. The child's face is not visible. This image is attached as EXHIBIT D.

c. CyberTipline Report# 47029044 was received by NCMEC on 02/23/2019 from MeetMe.com. MeetMe (Skout) reported possible child sex trafficking. On 02/21/2019 @ 19:37:21 UTC one (1) suspect image was uploaded by user "Tasha" (mayhemmason420@gmail.com) from IP address 209.42.155.219 (the PREMISES). The image was viewed by a SKOUT staff member. I reviewed the images included in this report and identified one (1) image of child pornography. The image is from the known series "Jewelry 1" (Exhibit B). There are also two (2) images of a female with her breasts exposed. It is difficult to determine the age of this female, although she appears to be a pubescent minor. The information received from SKOUT lists "Tasha" with a DOB of 01/04/1992. (As noted in paragraph 46(e) above, Mason STEPHENS DOB is 01/04/1992).

d. CyberTipline Report# 43568130 was received by NCMEC on 11/26/2018 from Facebook. Facebook reported possible possession, manufacture, and/or distribution of illegal content. On 11/25/2018 @ 04:10:38 UTC one (1) suspect image was received by user mason.stephens.3344 (mayhemmason420@gmail.com) at IP address 209.42.155.219 (the PREMISES). Facebook provided the associated name of Mason STEPHENS, DOB: 01/04/1992. The image was viewed by Facebook staff. I reviewed the image and it depicts a prepubescent female with the focal point on her vagina and anus. The child is spreading open her vagina with her hands. The child's breasts are exposed. The child has blonde/brown hair and lying on a bed with purple comforter and pink flowers. This image is attached as EXHIBIT E.

e. CyberTipline Report# 45679176 was received on 01/17/2019. This is the same information that was reported in NCMEC CyberTipline Report# 45679110.

53. On 05/17/2019, I issued a DHS Summons (ICE-HSI-MF-2019-00529) to Facebook for subscriber records for "steph.kuntz.90" On 05/28/2019, Facebook provided records identifying "Steph Keavy" with associated email address budnboobs420@gmail.com. Facebook provided IP logins from 02/24/2019 to 03/08/2019 and logouts from 02/24/2019 to 03/07/2019 from IP address 209.42.155.219 (the PREMISES).

54. On 06/14/2019, I met with TPD Detective Rideout and obtained records from TUMBLR relating to NCMEC CyberTipline report# 45415902. TUMBLR produced these records pursuant to a State Search Warrant. I reviewed the records, which includes the NCMEC known image of child pornography from the "At Sea" (Exhibit A) series distributed from the PREMISES.

55. In summary, The NCMEC reports associated to the IP address 209.42.155.219 (the PREMISES), subscribed to by Stephanie Stephens, at 57 Blueberry Lane, Apartment 28, Laconia, NH are associated with the possession/distribution of child pornography. The specific CyberTipline dates/times are:

43568130 (Facebook/1 unsubmitted image received) – 11/25/2018 @ 04:10:38 UTC

43568138 (Facebook/1 NCMEC known image received) - 11/25/2018 @ 04:23:19 UTC

45415902 (Tumblr/1 NCMEC known image uploaded) – 11/25/2018 @ 08:28:00 UTC

45690404 (Skout/1 NCMEC known image uploaded/1 unknown) – 12/20/2018

47029645 (MeetMe/1 NCMEC known image uploaded) – 02/21/2019 @ 06:07:39 UTC

47029044 (MeetMe/1 NCMEC known image uploaded) – 02-21-2019 @ 19:37:21 UTC

47028898 (MeetMe/1 NCMEC known image uploaded) – 02/21/2019 @ 19:46:24 UTC

47435362 (Facebook/1 unsubmitted image uploaded) – 03/08/2019 @ 10:20:18 UTC

CONCLUSION

56. Based on the aforementioned facts and circumstances, I respectfully submit that there is probable cause to believe the specified federal offenses occurred at the PREMISES; and that the fruits, evidence, and instrumentalities of those offenses are likely to be found at the PREMISES.

57. I, therefore, request that a search warrant be issued authorizing the search of the premises listed in Attachment A and the seizure of the items listed in Attachment B.

/s/ Ronald Morin
Ronald Morin
Special Agent
U.S. Department of Homeland Security
Immigration and Customs Enforcement
Homeland Security Investigations

Sworn and subscribed before me this 26th day of June 2019.

_____
HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF NEW HAMPSHIRE

I have reviewed the Exhibits referenced and I find probable cause to believe they depict minors engaging in sexually explicit conduct and child pornography. The Affiant shall preserve the images and video provided to the Court, for the duration of the pendency of this matter, including any relevant appeal process.

ATTACHMENT A

DESCRIPTION OF THE PREMISES

The address of 57 Blueberry Lane, Apartment 28, Laconia, NH 03246 is described as multi-family two (2) story building with eight (8) units per building. The building has tan vinyl siding with white trim. Apartment 28 is on the right corner of the building and the black numerals "28" are depicted on the right side of the white front entry door.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

Electronic and other communications pertaining to the solicitation, enticement, coercion, persuasion, inducement, and sexual exploitation of a minor; and images of child pornography and files containing images of child pornography in any form, wherever these items may be stored or found including, but not limited to:

1. Any computer equipment, computer, computer system and related peripherals, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, hardware and software operating manuals, tape systems and hard drive and other computer-related operation equipment, cellular phones, digital cameras, video cameras, scanners, computer photographs, graphic interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to, hardware, software, diskettes, backup tapes, CD-ROM's, DVD's, flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to visually depict child pornography or child erotica; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, and child erotica or information pertaining to an interest in child pornography, child erotica or information pertaining to an interest in child pornography or child erotica;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. Section 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256;

5. Information, electronic records, or correspondence pertaining to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

a. registries regarding peer-to-peer file-sharing software communications and participants in peer-to-peer file-sharing software networks;

b. envelopes, letters, and other correspondence including, but not limited to electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256; and

c. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. Section 2256;

6. Credit card information including but not limited to bills and payment records;

7. Records evidencing occupancy or ownership of the Premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

8. Records or other items that indicate ownership or use of computer equipment found in the Premises and/or Person, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes; and

9. Records, electronic or otherwise, or other items that relate to internet accounts and usernames, or any other groups that exhibit a sexual interest in children.

10. Contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical

locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If, after inspecting seized computer equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but

not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.